

Expert en cybersécurité

RNCP37832 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 326n
Formacode(s)	31045, 13235, 42881, 31038
Code(s) ROME	M1803, M1802, M1801, M1806, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	19/07/2023
Date d'échéance	19/07/2025

Certificateur(s)

YNOV · SIRET : 53056211500101

Partenaires habilités

20 organismes habilités, d'après la liste publiée par France compétences : 20 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
AIX YNOV CAMPUS	52831294500033	Former et organiser l'évaluation
BORDEAUX YNOV CAMPUS	53275739000036	Former et organiser l'évaluation
CONNECT YNOV CAMPUS	92042238300017	Former et organiser l'évaluation
DATASCIENTEST	83145006900024	Former et organiser l'évaluation
DATASCIENTEST	83145006900032	Former et organiser l'évaluation
DATASCIENTEST	83145006900040	Former et organiser l'évaluation
INSTITUT DE GESTION SOCIALE	31249509600140	Former et organiser l'évaluation
INSTITUT DE GESTION SOCIALE	31249509600165	Former et organiser l'évaluation
INSTITUT DE GESTION SOCIALE	31249509600173	Former et organiser l'évaluation
LILLE YNOV CAMPUS	90310559100023	Former et organiser l'évaluation

Liste complète des 20 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp37832-expert-en-cybersecurite/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'expert en sécurité informatique est un professionnel en capacité de paramétrer les systèmes de supervision de la sécurité (SIEM, sondes, honeypots, équipements filtrants). Il catégorise, analyse et traite les alertes de sécurité de façon régulière pour en améliorer l'efficacité. Il assure la détection, l'investigation et la réponse aux incidents de sécurité. Dans le domaine de la cybersécurité, il analyse et interprète les alertes, les événements corrélés et recherche les vulnérabilités. De manière générale, les opérateurs interprètent les événements de sécurité, écoutent le "bruit de fond" et traitent les alertes et les incidents.

ACTIVITÉS VISÉES

Mener une veille en cybersécurité

Etude de l'écosystème de l'organisation

Evaluation du niveau de sécurité de l'organisation et analyse du besoin de mise en conformité

Elaboration de la politique de sécurité du système d'information (PSSI)

Définition des outils destinés à garantir la disponibilité des données et à faciliter la résilience du système en cas d'incidents

A.2.1. Elaboration du plan d'actions de Sécurité

Déploiement des solutions de protection du SI

Déploiement des différents projets de sécurité conformément à la PSSI

Mise en place d'un processus de sensibilisation

Contrôle et Surveillance continue de la sécurité

Réalisation d'audit de sécurité

Analyse et qualification de l'incident

Développement et mise en œuvre des activités appropriées pour bloquer ou atténuer une menace ou intrusion (action de sauvegarde) / remédiation

Gestion des équipes en cas de crise

Communication de crise avec les parties prenantes

COMPÉTENCES ATTESTÉES

Organiser et animer un système de veille technique et technologique en matière de Sécurité du Système d'Information (SSI) à l'aide de recherches documentaires, de plateformes de partage, de webinars, de participations à des salons, des forums, clubs (CLUSIF, CLUSIR, ...etc.), afin d'être alerté des évolutions techniques, technologiques

Organiser et animer un système de veille réglementaire en matière de SSI en identifiant les sources de références du secteur de l'organisation afin de garantir la conformité de l'organisation à la réglementation

Organiser et animer un système de veille concernant les nouvelles menaces à l'aide de recherche Web, CERT afin d'être prévenu des alertes, vulnérabilités et menaces susceptibles d'impacter l'organisation

Traiter les informations recueillies en s'assurant de leur pertinence et véracité afin d'identifier les opportunités d'amélioration et obligations en matière de sécurité des données, des systèmes et des réseaux de l'organisation

Identifier les composants techniques et les différentes parties prenantes en étudiant l'écosystème afin d'établir la cartographie des informations, leur portée et les risques afférents.

Rédiger un état des lieux de l'exposition numérique de l'organisation à l'aide des données publiques disponibles sur internet afin d'identifier les risques en termes de sécurité et d'exigences réglementaires

Réaliser une analyse des risques en identifiant les événements pouvant affecter la sécurité du système d'information et en estimant les conséquences et les impacts potentiels afin de hiérarchiser les risques pouvant affecter le système d'information (SI)

Evaluer les besoins métier en consultant les utilisateurs et en identifiant les exigences fonctionnelles afin de déterminer les actions de sécurité à mettre en œuvre

Concevoir et rédiger des solutions techniques en étudiant le système d'information (SI) et les procédures informatiques d'une organisation afin de formaliser les objectifs de la stratégie de cybersécurité

Définir la politique de sécurité du système d'information (PSSI) en tenant compte de l'analyse de risques, du périmètre et des objectifs stratégiques de sécurité afin de s'assurer que les risques pesant sur le périmètre défini soient bien couverts

Identifier les moyens techniques et humains nécessaires à la mise en œuvre de la politique de sécurité du système d'information (PSSI) en prenant en compte la stratégie de l'organisation en termes de sécurité du SI afin de permettre une évaluation du coût de mise en œuvre de la PSSI

Estimer le coût de mise en œuvre de la politique de sécurité du système d'information (PSSI) en prenant en compte les différentes solutions possibles y compris assurantielles afin de permettre l'organisation de valider le déploiement des solutions

Elaborer les plans de sauvegarde, plan de secours informatique (PSI), plan de reprise d'activité (PRA), plan de continuité d'activité (PCA) en étudiant les processus et scénarios critiques afin de faciliter la résilience du système en cas d'incidents

Réaliser un processus de tests des PCA, PRA, PSI et plan de sauvegarde en simulant un incident afin de vérifier la capacité de l'organisation à les mettre en œuvre

Estimer les coûts associés à la mise en œuvre des PCA, PRA, PSI et plan de sauvegarde en identifiant l'ensemble des postes de dépenses afin d'intégrer ces coûts dans le budget de l'organisation

Décliner la politique de sécurité du système d'information (PSSI) en actions et/ou règles de sécurité adaptées à la cible en prenant en compte l'état actuel du système d'information (SI) afin de déterminer les impacts sur l'organisation
Elaborer le plan d'actions en priorisant les actions selon les enjeux de sécurité identifiés et en évaluant leurs coûts afin d'éclairer la prise de décision.

Rédiger le corpus documentaire en tenant compte de la politique de sécurité du système d'information (PSSI) afin d'encadrer l'utilisation /l'usage du système d'information (SI)

Concevoir une architecture sécurisée en utilisant les méthodes et solutions connues afin de garantir la sécurité du système d'information (SI)

Rationaliser les identités et les accès à l'aide de différents dispositifs de contrôle et d'alerte (électronique, physique et informatique) afin d'éviter les diffusions d'informations indues

Mettre en place les solutions potentielles de sécurité (VPN, chiffrement de portable, protection de fichiers, ...) en identifiant les besoins (classification et usage) afin de renforcer la protection des informations contre les accès indus et risques de divulgation accidentelle ou malveillante

Intégrer la sécurité dans l'organisation en appliquant les prérequis, les normes et les bonnes pratiques en matière de sécurisation du système d'information (SI) en vigueur, afin de garantir un niveau de sécurité en adéquation avec la PSSI

Définir un processus de validation des changements en évaluant la demande de changement, en analysant son impact et en accompagnant les parties prenantes aux changements afin de garantir la sécurité du système d'information (SI) dans le déploiement des projets

Elaborer les spécifications fonctionnelles d'un projet de sécurité en tenant compte de l'exposition au risque, des ressources nécessaires et de la politique de sécurité du système d'information (PSSI) afin de définir les spécifications techniques

Planifier un projet de sécurité du système d'information (SI) en tenant compte des ressources humaines, matérielles, financières nécessaires à l'exécution du projet afin de définir l'ordonnancement détaillé des tâches, clarifier les responsabilités des différents acteurs et assurer une bonne coordination

Piloter l'avancement d'un projet après avoir défini les outils de suivi adaptés, en assurant un suivi régulier de l'avancée, en communiquant sur les indicateurs clés afin de garantir la performance du projet dans le respect des délais, de la qualité et des coûts

Réaliser une campagne de tests conformément au cahier de recettes afin de s'assurer que le projet réponde aux attentes et spécifications définies

Rédiger la documentation projet en tenant compte des spécificités du projet et son impact dans l'organisation du système d'information (SI) afin de permettre la livraison du projet

Elaborer une politique de sensibilisation aux risques de cybersécurité en impliquant tous les collaborateurs afin de prévenir les incidents de cybersécurité au sein de l'organisation

Déployer la politique de sensibilisation aux risques de cybersécurité en élaborant des supports et des méthodes de formation afin d'aider les utilisateurs du système d'information (SI) à s'approprier la culture de cybersécurité mise en place

Mettre en place une politique de contrôle et de surveillance continue en tenant compte des menaces identifiées et de la PSSI afin de s'assurer de l'efficacité des mesures de protection

Identifier, en étudiant le contexte du système d'information, les paramètres à connaître et mesurer, qui permettent soit par leur valeur absolue, soit par leur variation d'évaluer le niveau de sécurité du système d'information

Mettre en place une surveillance et un contrôle à l'aide de dispositifs de sécurité et d'outils de supervision afin de s'assurer du fonctionnement continu et efficace des dispositifs de sécurité mis en place

Documenter les vulnérabilités détectées par les moyens techniques de surveillance en analysant les risques associés afin de décrire les mesures à prendre

Corriger les vulnérabilités identifiées en élaborant un plan d'actions approprié afin de restaurer la sécurité du système concerné

Définir le plan d'audit en délimitant le périmètre à étudier et en prenant en compte les points critiques afin de s'assurer de la bonne application des politiques et procédures de sécurité

Rédiger un rapport d'audit en précisant la démarche suivie, les actions entreprises les vulnérabilités détectées afin d'établir un plan de remédiation

Suivre la mise en œuvre des actions correctives en vérifiant leur efficacité afin d'augmenter la sécurité de l'organisation

Identifier les incidents de sécurité détectés à l'aide des outils de supervision au sein d'un Security Operations Center (SOC) afin de permettre leur analyse

Réaliser une analyse forensique de l'incident en collectant les preuves afin de permettre la présentation d'une synthèse destinée aux décideurs

Utiliser des moyens d'atténuation, de réparation ou de récupération du système d'information (SI), en utilisant des outils dédiés afin d'assurer la continuité du bon fonctionnement du SI et la préservation des données

Réaliser un protocole de tests afin de vérifier que les moyens et solutions techniques mis en œuvre permettent de corriger une faille informatique

Mettre en œuvre le plan de restauration du SI en utilisant des solutions techniques afin de restaurer toutes les capacités ou les Services du système d'information (SI)

Donner des instructions et un plan d'actions détaillé pour répondre aux intrusions en maintenant la communication avec les équipes et la direction afin de piloter la gestion de crise

Définir un plan de communication de crise en identifiant les parties prenantes à informer et les canaux de communication à utiliser afin de réagir de manière efficace en cas de crise

Présenter une synthèse de l'incident à partir des éléments présents dans le rapport d'analyse forensique afin de faire valider les adaptations des procédures du système d'information (SI) à déployer

Blocs de compétences

RNCP37832BC01 — Définir la stratégie de cybersécurité d'une organisation

LISTE DE COMPÉTENCES

Organiser et animer un système de veille technique et technologique en matière de Sécurité du Système d'Information (SSI) à l'aide de recherches documentaires, de plateformes de partage, de webinars, de participations à des salons, des forums, clubs (CLUSIF, CLUSIR, ...etc.), afin d'être alerté des évolutions techniques, technologiques

Organiser et animer un système de veille réglementaire en matière de sécurité du système d'information (SSI) en identifiant les sources de références du secteur de l'organisation afin de garantir la conformité de l'organisation à la réglementation

Organiser et animer un système de veille concernant les nouvelles menaces à l'aide de recherche Web, CERT afin d'être prévenu des alertes, vulnérabilités et menaces susceptibles d'impacter l'organisation

Traiter les informations recueillies en s'assurant de leur pertinence et véracité afin d'identifier les opportunités d'amélioration et obligations en matière de sécurité des données, des systèmes et des réseaux de l'organisation

Identifier les composants techniques et les différentes parties prenantes en étudiant l'écosystème afin d'établir la cartographie des informations, leur portée et les risques afférents

Rédiger un état des lieux de l'exposition numérique de l'organisation à l'aide des données publiques disponibles sur internet afin d'identifier les risques en termes de sécurité et d'exigences réglementaires

Réaliser une analyse des risques en identifiant les événements pouvant affecter la sécurité du système d'information et en estimant les conséquences et les impacts potentiels afin de hiérarchiser les risques pouvant affecter le système d'information (SI)

Evaluer les besoins métier en consultant les utilisateurs et en identifiant les exigences fonctionnelles afin de déterminer les actions de sécurité à mettre en œuvre

Concevoir et rédiger des solutions techniques en étudiant le système d'information (SI) et les procédures informatiques d'une organisation afin de formaliser les objectifs de la stratégie de cybersécurité

Définir la politique de sécurité du système d'information (PSSI) en tenant compte de l'analyse de risques, du périmètre et des objectifs stratégiques de sécurité afin de s'assurer que les risques pesant sur le périmètre défini soient bien couverts

Identifier les moyens techniques et humains nécessaires à la mise en œuvre de la PSSI en prenant en compte la stratégie de l'organisation en termes de sécurité du SI afin de permettre une évaluation du coût de mise en œuvre de la PSSI

Estimer le coût de mise en œuvre de la PSSI en prenant en compte les différentes solutions possibles y compris assurantielles afin de permettre l'organisation de valider le déploiement des solutions

Elaborer les plans de sauvegarde, plan de secours informatique (PSI) , plan de reprise d'activité (PRA), plan de continuité d'activité (PCA) en étudiant les processus et scénarios critiques afin de faciliter la résilience du système en cas d'incidents

Réaliser un processus de tests des PCA, PRA, PSI et plan de sauvegarde en simulant un incident afin de vérifier la capacité de l'organisation à les mettre en œuvre

Estimer les coûts associés à la mise en œuvre des PCA, PRA, PSI en identifiant l'ensemble des postes de dépenses

afin d'intégrer ces coûts dans le budget de l'organisation

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle réelle ou fictive avec rendus de livrables

RNCP37832BC02 — Elaborer et piloter des processus de cybersécurité d'une organisation

LISTE DE COMPÉTENCES

Décliner la Politique de sécurité du système d'information (PSSI) en actions et/ou règles de sécurité adaptées à la cible en prenant en compte l'état actuel du système d'information (SI) afin de déterminer les impacts sur l'organisation
Elaborer le plan d'actions en priorisant les actions selon les enjeux de sécurité identifiés et en évaluant leurs coûts afin d'éclairer la prise de décision

Rédiger le corpus documentaire en tenant compte de la Politique de sécurité du système d'information (PSSI) afin d'encadrer l'utilisation /l'usage du système d'information (SI)

Concevoir une architecture sécurisée en utilisant les méthodes et solutions connues afin de garantir la sécurité du système d'information (SI)

Rationaliser les identités et les accès à l'aide de différents dispositifs de contrôle et d'alerte (électronique, physique et informatique) afin d'éviter les diffusions d'informations indues

Mettre en place les solutions potentielles de sécurité (VPN, chiffrement de portable, protection de fichiers, ...) en identifiant les besoins (classification et usage) afin de renforcer la protection des informations contre les accès indus et risques de divulgation accidentelle ou malveillante

Intégrer la sécurité dans l'organisation en appliquant les prérequis, les normes et les bonnes pratiques en matière de sécurisation du système d'information (SI) en vigueur, afin de garantir un niveau de sécurité en adéquation avec la Politique de sécurité du système d'information (PSSI)

Définir un processus de validation des changements en évaluant la demande de changement, en analysant son impact et en accompagnant les parties prenantes aux changements afin de garantir la sécurité du système d'information (SI) dans le déploiement des projets

Elaborer les spécifications fonctionnelles d'un projet de sécurité en tenant compte de l'exposition au risque, des ressources nécessaires et de la politique de sécurité du système d'information (PSSI) afin de définir les spécifications techniques

Planifier un projet de sécurité du système d'information (SI) en tenant compte des ressources humaines, matérielles, financières nécessaires à l'exécution du projet afin de définir l'ordonnancement détaillé des tâches, clarifier les responsabilités des différents acteurs et assurer une bonne coordination

Piloter l'avancement d'un projet après avoir défini les outils de suivi adaptés, en assurant un suivi régulier de l'avancée, en communiquant sur les indicateurs clés afin de garantir la performance du projet dans le respect des délais, de la qualité et des coûts

Réaliser une campagne de tests conformément au cahier de recettes afin de s'assurer que le projet réponde aux attentes et spécifications définies

Rédiger la documentation projet en tenant compte des spécificités du projet et son impact dans l'organisation du système d'information (SI) afin de permettre la livraison du projet

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle réelle ou fictive avec rendus de livrables et soutenance orale devant jury

RNCP37832BC03 — Maintenir la sécurité du système d'information d'une organisation

LISTE DE COMPÉTENCES

Elaborer une politique de sensibilisation aux risques de cybersécurité en impliquant tous les collaborateurs afin de prévenir les incidents de cybersécurité au sein de l'organisation

Déployer la politique de sensibilisation aux risques de cybersécurité en élaborant des supports et des méthodes de formation afin d'aider les utilisateurs du système d'information (SI) à s'approprier la culture de cybersécurité mise en place

Mettre en place une politique de contrôle et de surveillance continue en tenant compte des menaces identifiées et de la PSSI afin de s'assurer de l'efficacité des mesures de protection

Identifier, en étudiant le contexte du système d'information, les paramètres à connaître et mesurer, qui permettent soit par leur valeur absolue, soit par leur variation d'évaluer le niveau de sécurité du système d'information

Mettre en place une surveillance et un contrôle à l'aide de dispositifs de sécurité et d'outils de supervision afin de s'assurer du fonctionnement continu et efficace des dispositifs de sécurité mis en place

Documenter les vulnérabilités détectées par les moyens techniques de surveillance en analysant les risques associés afin de décrire les mesures à prendre

Corriger les vulnérabilités identifiées en élaborant un plan d'actions approprié afin de restaurer la sécurité du système concerné

Définir le plan d'audit en délimitant le périmètre à étudier et en prenant en compte les points critiques afin de s'assurer de la bonne application des politiques et procédures de sécurité

Rédiger un rapport d'audit en précisant la démarche suivie, les actions entreprises les vulnérabilités détectées afin d'établir un plan de remédiation

Suivre la mise en œuvre des actions correctives en vérifiant leur efficacité afin d'augmenter la sécurité de l'organisation

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle réelle ou fictive avec rendus de livrables et soutenance orale devant jury

RNCP37832BC04 — Gérer les incidents et crises de cybersécurité d'une organisation :

LISTE DE COMPÉTENCES

Identifier les incidents de sécurité détectés à l'aide des outils de supervision au sein d'un Security Operations Center (SOC) afin de permettre leur analyse

Réaliser une analyse forensique de l'incident en collectant les preuves afin de permettre la présentation d'une synthèse destinée aux décideurs

Utiliser des moyens d'atténuation, de réparation ou de récupération du système d'information (SI), en utilisant des outils dédiés afin d'assurer la continuité du bon fonctionnement du SI et la préservation des données

Réaliser un protocole de tests afin de vérifier que les moyens et solutions techniques mis en œuvre permettent de corriger une faille informatique

Mettre en œuvre le plan de restauration du SI en utilisant des solutions techniques afin de restaurer toutes les capacités ou les Services du système d'information (SI)

Donner des instructions et un plan d'actions détaillé pour répondre aux intrusions en maintenant la communication avec les équipes et la direction afin de piloter la gestion de crise

Définir un plan de communication de crise en identifiant les parties prenantes à informer et les canaux de communication à utiliser afin de réagir de manière efficace en cas de crise

Présenter une synthèse de l'incident à partir des éléments présents dans le rapport d'analyse forensique afin de faire valider les adaptations des procédures du système d'information (SI) à déployer

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle réelle ou fictive avec rendus de livrables

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'expert en cybersécurité peut intégrer tous types de structures (entreprise, organisation, administration, freelance) de tous secteurs confondus (industrie, énergie, télécommunications, acteurs du e-commerce, constructeurs informatiques, administration, banques, services, transport, santé, éducation, ...).

TYPE D'EMPLOIS ACCESSIBLES

- Ingénieur cybersécurité
- Consultant en cybersécurité ;
- Auditeur sécurité des systèmes d'informations
- Architecte sécurité des systèmes d'information
- Expert en sécurité des systèmes d'information
- Spécialiste en cybersécurité ;
- Analyste SOC Security Operations Center.
- Pentester
- Chef de projet en sécurité des systèmes d'information

RÈGLEMENTATIONS D'ACTIVITÉ

Le métier d'expert en cybersécurité n'est pas réglementé, néanmoins les activités de l'expert en Cybersécurité s'inscrivent dans un cadre légal et réglementaire en constante évolution, que cela soit de manière globale ou

spécifique à certains secteurs, national, européen ou international.

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 942 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (19 % des actifs en emploi)
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (Élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	16 497
Jugés difficiles à recruter	46 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X91 — Chefs de projet et directeurs de service informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Le dispositif s'adresse aux titulaires d'un baccalauréat ou d'un diplôme équivalent de niveau 4.

Dans le cadre d'admission parallèle :

être titulaire d'un diplôme ou titre de niveau 5 ou équivalent dans le domaine de l'informatique : intégration en 3ème année

être titulaire d'un diplôme ou titre de niveau 6 ou équivalent dans le domaine de l'informatique : intégration en 4ème année

être titulaire d'un diplôme ou titre de niveau 6 correspondant à un bac+4 ou équivalent dans le domaine de l'informatique : intégration en 5ème année.

Toute demande ne répondant pas aux prérequis de la formation est étudiée par une commission placée sous l'autorité du certificateur.

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION

Le jury de certification est composé de 5 membres dont 3 professionnels externes

COMPOSITION DU JURY — VAE

Le jury de certification est composé de 5 membres dont 3 professionnels externes

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	9 157 €
Selon la branche	8 000 € – 12 000 €
Prise en charge	Branches concernées
9 157 €	Valeur par défaut · 168 branches
12 000 €	CPNE Entreprises des activités du déchet et de la propreté urbaine, CPNE autoroutes, CPNE de l'ingénierie, des services informatiques et du conseil, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des exploitations frigorifiques
8 740 €	CNPEFP des sociétés d'assistance, CPNEFP de la branche professionnelle des Entreprises du courtage d'assurances et/ou réassurances, CPNFPE des sociétés d'assurances
8 696 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP des jardineries et graineteries, CPNEFP du Négoce de l'ameublement
11 250 €	CPNE de la branche de la Distribution Directe, CPNEF de l'Exploitation cinématographique et de la Distribution de films
10 683 €	CPNEFP de l'enseignement privé indépendant, CPNEFP de la Restauration rapide
10 000 €	CPNE des industries de santé (CPNEIS), Commission Paritaire Activités de Marchés Financiers
9 992 €	CPNEF branche retraite complémentaire et prévoyance, CPNEFP Mutualité
9 500 €	CPNE Branche Caisse d'Epargne, CPNE de la branche Banque Populaire
9 000 €	CPNE Banque, CPNEFP de la branche des prestataires de services du secteur tertiaire
11 447 €	CPNE des Télécoms
11 446 €	CPNE Travail Temporaire
11 258 €	CPNEFP de la Mutualité Sociale Agricole
10 500 €	CPNEFP des industries des tuiles et briques
10 164 €	CPNE Casinos
9 800 €	CPNEF de l'audiovisuel
9 231 €	CPNEFP Commerce à distance
8 942 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 701 €	CPNE FP Branche des magasins du Bricolage
8 520 €	CPNE de la branche des experts comptables et commissaires aux comptes
8 500 €	CPNEFP de la métallurgie
8 000 €	CPNE chimie

Base légale

Date de décision	19/07/2023
Durée de l'enregistrement	2 ans

Date d'échéance de l'enregistrement	19/07/2025
Date de dernière délivrance possible	19/07/2029

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2022	50	0	92 %	—
2021	32	0	97 %	—
2020	35	0	91 %	92 %
2019	25	0	96 %	90 %

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP40897

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
Alternance Cybersécurité - Ynov

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37832/>

Entrées et sorties de formation

Entrées en formation	39
Parcours menés à terme	29
Taux d'achèvement	74 %
Période	09/2024 – 05/2026

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	46
Montant total engagé	200 652 €
Coût moyen par dossier	4 362 €
Durée moyenne	602 h
Période	06/2024 – 07/2025
France compétences	64 %
France Travail	14 %
OPCO	11 %
Entreprise	9 %
Reste à charge titulaire	2 %

